

# PATENT ABSTRACTS OF JAPAN

(11) Publication number : 09-152990  
(43) Date of publication of application : 10. 06. 1997

(51) Int. Cl. G06F 12/14  
G06F 12/14  
G06F 12/00  
G06F 15/00

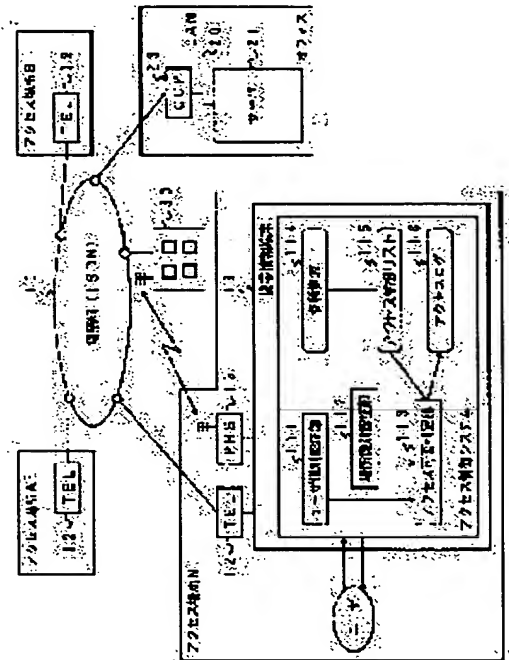
(21) Application number : 07-312592 (71) Applicant : TOSHIBA CORP  
(22) Date of filing : 30. 11. 1995 (72) Inventor : YOSHINO YASUAKI

## (54) ACCESS CONTROL SYSTEM AND ITS METHOD

**(57) Abstract:**

**PROBLEM TO BE SOLVED:** To attain an access control system for obtaining security optimum to a mobile computing environment.

**SOLUTION:** An access place for utilizing an information terminal 11 is specified by a place identifying/certificating part 112 and an access control list 115 is searched by the specified information security level. An information security level necessary for accessing each resource is regulated in the list 115. Consequently, an access place requested by a user can be added to an access availability judging reference and restriction to resources to be utilized can be changed in accordance with the access place.



**LEGAL STATUS**

[Date of request for examination]  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

Copyright (C) ; 1998, 2003 Japan Patent Office

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-152990

(43) 公開日 平成9年(1997)6月10日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 1 0		G 0 6 F 12/14	3 1 0 K
	3 2 0			3 2 0 A
12/00	5 3 7		12/00	5 3 7 A
15/00	3 3 0		15/00	3 3 0 D

審査請求 未請求 請求項の数 9 O L (全 16 頁)

(21) 出願番号 特願平7-312592

(22) 出願日 平成7年(1995)11月30日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 吉野 恭明

東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

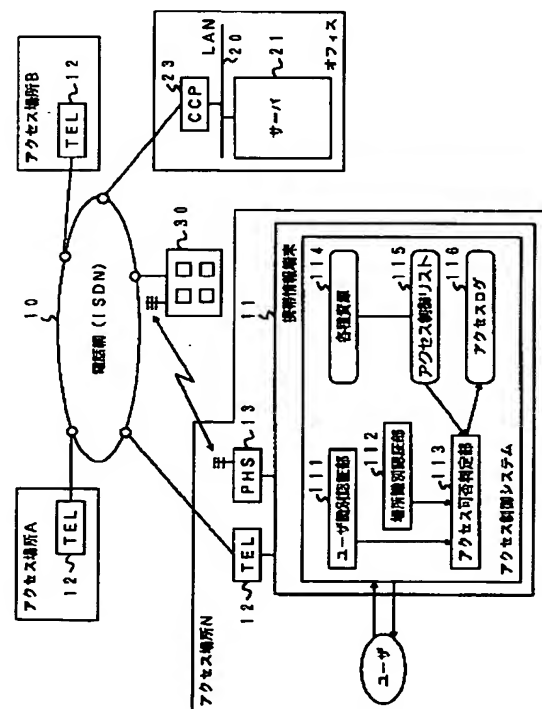
(74) 代理人 弁理士 鈴江 武彦

## (54) 【発明の名称】 アクセス制御システムおよびアクセス制御方法

## (57) 【要約】

【課題】 モバイルコンピューティング環境に最適なセキュリティ確保のためのアクセス制御システムを実現する。

【解決手段】 情報端末 11 を利用するアクセス場所が場所識別認証部 112 によって特定され、その特定された情報セキュリティレベルを用いて、アクセス制御リスト 115 がサーチされる。アクセス制御リスト 115 には、資源毎にそれをアクセスするために必要な情報セキュリティレベルが規定されている。従って、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようになり、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。



## 1

## 【特許請求の範囲】

【請求項 1】 各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、  
前記資源のアクセスのために利用者によって情報端末が使用されるアクセス場所を特定するアクセス場所特定手段と、

このアクセス場所特定手段によって特定されたアクセス場所に対して予め設定されている情報セキュリティレベルに応じて、前記利用者から要求された資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備することを特徴とするアクセス制御システム。

【請求項 2】 前記アクセス可否判定手段は、  
各資源とその資源をアクセスするために必要なアクセス場所の情報セキュリティレベルとの対応関係を規定したアクセス制御リストを有し、  
このアクセス制御リストの内容と、前記アクセス場所特定手段によって特定されたアクセス場所の情報セキュリティレベルとに従って、前記利用者から要求された資源に対するアクセスの可否を判定することを特徴とする請求項 1 記載のアクセス制御システム。

【請求項 3】 前記アクセス場所特定手段は、  
利用者によって情報端末が使用されるアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従ってアクセス場所を特定することを特徴とする請求項 1 記載のアクセス制御システム。

【請求項 4】 前記通信装置は、  
その通信装置が設置されているアクセス場所を示す識別子を暗号化して発生し、  
前記情報セキュリティレベル検出手段は、前記暗号化された識別子を復号化して前記アクセス場所を特定することを特徴とする請求項 3 記載のアクセス制御システム。

【請求項 5】 携帯情報端末を用いたモバイルコンピューティング環境下で、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、  
利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従って前記携帯情報端末が使用されるアクセス場所の情報セキュリティレベルを検出する情報セキュリティレベル検出手段と、  
各資源とその資源をアクセスするために必要な情報セキュリティレベルとの対応関係を規定したアクセス制御リストと、前記情報セキュリティレベル検出手段によって検出された前記アクセス場所の情報セキュリティレベルとに従って、前記利用者から要求された前記携帯情報端末内の資源、または前記携帯情報端末と通信媒体を介して接続可能な他の情報処理装置内の資源に対するアクセスの可否を判定するアクセス可否判定手段とを具

## 2

備することを特徴とするアクセス制御システム。

【請求項 6】 携帯情報端末と、通信媒体を介して前記携帯情報端末と各種情報を授受するサーバ計算機とを利用したモバイルコンピューティング環境下で、前記サーバ計算機内の各種コンピュータ資源に対する前記携帯情報端末の利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、前記携帯情報端末は、

利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従って前記携帯情報端末が使用されるアクセス場所の情報セキュリティレベルを検出する情報セキュリティレベル検出手段を具備し、

前記サーバ計算機は、  
各資源とその資源をアクセスするために必要な情報セキュリティレベルとの対応関係を規定したアクセス制御リストを保持する手段と、

前記携帯情報端末の前記情報セキュリティレベル検出手段によって検出された前記アクセス場所の情報セキュリティレベルと、前記アクセス制御リストとに従って、前記携帯情報端末から要求された前記サーバ計算機内の資源に対するアクセス要求の可否を判定する手段とを具備することを特徴とするアクセス制御システム。

【請求項 7】 携帯情報端末と、通信媒体を介して前記携帯情報端末と各種情報を授受するサーバ計算機とを利用したモバイルコンピューティング環境下で、前記サーバ計算機内の各種コンピュータ資源に対する前記携帯情報端末の利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、前記携帯情報端末は、

前記サーバ計算機から提供された資源を保持し、その運用および管理を行うキャッシュ管理手段と、

利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所に設置された通信装置から発生される信号を受信し、その受信信号に従って前記携帯情報端末が使用されるアクセス場所の情報セキュリティレベルを検出する情報セキュリティレベル検出手段と、

各資源とその資源をアクセスするために必要な情報セキュリティレベルとの対応関係を規定したアクセス制御リストと、前記情報セキュリティレベル検出手段によって検出された前記アクセス場所の情報セキュリティレベルとに従って、前記利用者から要求された前記キャッシュ管理装置内の資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備し、

前記サーバ計算機は、  
各資源とその資源をアクセスするために必要な情報セキュリティレベルとの対応関係を規定したアクセス制御リストを保持する手段と、

前記携帯情報端末の前記情報セキュリティレベル検出手段によって検出された前記アクセス場所の情報セキュ

## 3

リティーレベルと、前記アクセス制御リストとに従って、前記携帯情報端末から要求された前記キャッシュ管理部に存在していない前記サーバ計算機内の資源に対するアクセス要求の可否を判定する手段とを具備することを特徴とするアクセス制御システム。

【請求項 8】 携帯情報端末を用いたモバイルコンピューティング環境下で、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御方法において、利用者が携帯情報端末を用いてアクセス操作を行うアクセス場所の情報セキュリティレベルを検出し、この検出された前記アクセス場所の情報セキュリティレベルに従って、前記利用者から要求された資源に対するアクセスの可否を判定し、アクセス場所に依じて利用可能な資源を制限することを特徴とするアクセス制御方法。

【請求項 9】 携帯情報端末を用いたモバイルコンピューティング環境下で、利用者が前記携帯情報端末を用いてアクセス操作を行うアクセス場所に依じて、前記携帯情報端末の利用者からのコンピュータ資源に対するアクセス要求を許可または禁止するアクセス制御方法であって、前記携帯情報端末が利用されるアクセス場所毎にそのアクセス場所に対応する情報セキュリティレベルを示す電波環境を提供し、その電波環境下におかれた前記携帯情報端末がその電波を受信することによって、その携帯情報端末が利用されるアクセス場所の情報セキュリティレベルを検出し、その検出された情報セキュリティレベルを用いることにより、アクセス場所に依じて利用可能な資源を制限できるようにしたことを特徴とするアクセス制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムおよびアクセス制御方法に関する。

【0002】

【従来の技術】 近年、コンピュータやネットワーク技術の発達、あるいはそれらを利用した情報サービスの発展に伴い、様々な情報セキュリティ技術が実現されている。この情報セキュリティを実現する技術の 1 つとして、アクセス制御が知られている。

【0003】 アクセス制御とは、ユーザ認証などにより識別された主体から要求されたコンピュータ資源へのアクセスを、予め設定されたアクセス制御リストを用いて許可するか禁止するかの制御を行う技術をいう。アクセス制御リストには、ユーザ名とそのユーザが利用可能な資源との対応関係などが記述されている。

【0004】 このアクセス制御技術を利用することによ

## 4

り、特定個人／特定計算機の関係において特定資源の利用だけを許可するという情報セキュリティが実現され、悪意を持った様々な不正アクセスからコンピュータ資源を保護することができる。

【0005】 しかし、PDA、サブノート PC 等の携帯情報端末を用いるモバイルコンピューティング環境下においては、個人や計算機の情報だけでアクセス可否を判断する従来のアクセス制御技術では、十分な情報セキュリティを得ることはできない。

【0006】 すなわち、モバイルコンピューティング環境下では、個人が携帯情報端末を持ち歩いて、不特定の場所からその携帯情報端末内のデータを直接アクセスしたり、遠隔地にあるサーバ計算機のデータベースなどにネットワーク経由でアクセスする可能性がある。この場合、その携帯情報端末が使用される場所によっては、サーバから提供された機密性を持つ情報や個人認証のためのパスワードが第三者に盗まれたり、その情報漏洩が元で、ネットワークを介したサーバ計算機への不正進入を許し、機密情報の改竄や運用妨害といった攻撃を受ける危険がある。

【0007】 また、最近では、携帯情報端末自体から発生される電磁波から、その携帯情報端末の表示画面の内容や操作状況を読みとることができるという報告もなされている。したがって、モバイルコンピューティング環境下では、携帯情報端末を使用する場所そのものが、セキュリティ保持のための重要な要素となっている。

【0008】

【発明が解決しようとする課題】 上述したように、モバイルコンピューティング環境下では、個人が携帯情報端末を持ち歩いて、不特定の場所からその携帯情報端末内のデータを直接アクセスしたり、遠隔地にあるサーバ計算機のデータベースなどにネットワーク経由でアクセスする可能性があるため、個人や計算機の情報だけでアクセス可否を判断する従来のアクセス制御技術では、十分な情報セキュリティを得ることができないという問題がある。

【0009】 この発明はこの様な点に鑑みてなされたものであり、個人や計算機の情報だけでなく、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようにして、十分なセキュリティを確保しながらユーザの利便を考慮したアクセス形態を実現し得るアクセス制御システムおよびアクセス制御方法を提供することを目的とする。

【0010】

【課題を解決するための手段】 この発明は、各種コンピュータ資源に対する利用者からのアクセス要求を許可または禁止するための制御を行うアクセス制御システムにおいて、前記資源のアクセスのために利用者によって情報端末が使用されるアクセス場所を特定するアクセス場所特定手段と、このアクセス場所特定手段によって特定

されたアクセス場所について予め設定された情報セキュリティレベルに応じて、前記利用者から要求された資源に対するアクセスの可否を判定するアクセス可否判定手段とを具備することを特徴とする。

【0011】このアクセス制御システムにおいては、情報端末を利用するアクセス場所が特定され、そのアクセス場所の情報セキュリティレベルを使用したアクセス制御が行われる。このため、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようになり、アクセス場所に応じて、利用できる資源の制限

を変えることが可能となる。

【0012】従って、公共の場所などのようにセキュリティレベルが低い場所では機密性の高い情報へのアクセスは禁止されるが、外出先であっても、セキュリティレベルが高い場所であれば、機密情報にアクセスすることができる。よって、十分なセキュリティを確保しながらユーザの利便を考慮したアクセス形態を実現できる。

【0013】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図1には、この発明の一実施形態に係るアクセス制御システムが適用されるモバイルコンピューティングシステム全体の構成が示されている。このモバイルコンピューティングシステムは、携帯情報端末11と、この携帯情報端末11と電話回線網やISDNなどの通信網10を介して各種情報を授受するサーバ計算機21とを利用して実現されている。

【0014】携帯情報端末11は例えばPDAやノートPC等の小型電子機器であり、自宅、マンション、自社オフィス、サテライトオフィス、貸しオフィス、ホテル、喫茶店、公園、空港、地下鉄など、不特定の場所（アクセス場所A、B、…、N）で利用される。この携帯情報端末11はその端末11内の記憶装置に対する情報の入出力を始め、通信網10を経由してサーバ計算機21をアクセスするための通信機能も有している。携帯情報端末11の利用者が外出先などからサーバ計算機21と通信する場合には、その利用者が現在いる場所に設置されている電話機12等の公衆通信端末に携帯情報端末11が接続され、有線通信の形態で携帯情報端末11とサーバ計算機21間の通信が行われる。また、PHS13等の携帯電話を使用すれば、電話機12がない場所でも、最寄りの無線電話基地局30経由でサーバ計算機21と通信することができる。

【0015】サーバ計算機21は、例えばオフィス内等に配置されている計算機であり、LAN20および通信制御装置(CCP)23等を介して通信回線網10と接続されている。

【0016】この実施形態では、携帯情報端末11内に次のようなアクセス制御システムが実現されている。このアクセス制御システムは、携帯情報端末11内の各種

資源114に対する利用者からのアクセス要求を許可または禁止するための制御を行うソフトウェアであり、ユーザ識別認証部111、アクセス場所識別認証部112、アクセス可否判定部113、アクセス制御リスト115、およびアクセスログ116を備えている。

【0017】ユーザ識別認証部111は、携帯情報端末11の利用者によって入力されるユーザ名を使用して利用者が誰であるかを識別し、次いで、そのユーザ名に対応する登録パスワードと利用者によって入力されるパスワードとの照合を行って、利用者が正当な人であることを調べるための認証を行う。

【0018】アクセス場所識別認証部112は、携帯情報端末11が現在利用されているアクセス場所およびそのアクセス場所について予め設定された情報セキュリティレベルについてその識別および認証を行う。このアクセス場所識別認証部112による場所に関する識別および認証処理の原理を図2に示す。

【0019】図2に示されているように、例えば、貸しオフィス、ホテル、喫茶店、各種交通機関等に構築された各アクセス場所においては、セキュリティレベル発信器100が予め設置されており、そのセキュリティレベル発信器100から送信される電波等の無線信号が携帯情報端末11によって受信される。

【0020】セキュリティレベル発信器100から携帯情報端末11の場所識別認証部112に与えられる情報は、そのアクセス場所を特定するための識別子とそのアクセス場所に対して予め設定された情報セキュリティレベルである。

【0021】各アクセス場所の情報セキュリティレベルは、公共的な中立機関によって定めた基準に従って決定する。すなわち、中立機関は、アクセス場所毎にそのアクセス場所の環境を評価し、基準に従ってそのアクセス場所の情報セキュリティレベルを認定する。情報セキュリティレベルは、セキュリティに関して何も考慮されていない最低レベルから、ソフト／ハード両側面から最大級の対策が施されている最高レベルまで、複数の段階に区分される。これにより、自宅、自社オフィス、サテライトオフィス、貸しオフィス、ホテル、喫茶店、各種交通機関等においては、用途／予算に応じて、様々なセキュリティレベルの「アクセス場所」を構築することができる。

【0022】情報セキュリティレベルの認定がなされたアクセス場所に対しては、その場所の識別子と認定された情報セキュリティレベルの情報とが設定されたセキュリティレベル発信器100が付与される。

【0023】この場合、セキュリティレベル発信器100から発生される情報の改竄を防止するために、セキュリティレベル発信器100に設定される情報は中立機関によって電子署名などの暗号技術を用いて暗号化されて保護されている。従って、セキュリティレベル発

10

20

30

40

50

信器100からも暗号化された信号が発生されることになる。携帯情報端末11は、この暗号化された信号を復号化してアクセス場所の識別子および情報セキュリティレベルを認識する。

【0024】図3には、セキュリティレベル発信器100から発生されるセキュリティレベル信号の内容とセキュリティレベルの高低との対応関係が示されている。この例では、セキュリティレベル信号Aが最もセキュリティが高く、セキュリティレベル信号B、C、D、E、Fの順でセキュリティレベルが段階的に低くなる。また、場所識別子や情報セキュリティレベルについての情報が得られない場所は、場所不明、且つ最低レベルのセキュリティとして扱われる。

【0025】以上のように、場所識別認証部112は、携帯情報端末11が存在するアクセス場所の電波環境からその場所とその場所の情報セキュリティレベルを決定する。

【0026】次に、図1のアクセス制御システムの他の構成要素について説明する。アクセス可否判定部113は、ユーザ識別認証部111および場所識別認証部112それぞれからの識別認識情報と、アクセス制御リスト115の内容に従って、ユーザから要求された資源に対するアクセスを許可するか否かの可否判定を行う。この判定結果は、アクセス制御の履歴情報としてアクセスログ116に記録される。この履歴情報は、攻撃行為の検出や攻撃者の特定などに使用される。

【0027】アクセス制御リスト115は、各種資源114それぞれについて、それをアクセス可能なユーザ名（またはグループ名）とアクセス場所の情報セキュリティレベルを規定したものであり、図4に示されているように、資源、ユーザ名（またはグループ名）、および情報セキュリティレベルの対応関係が保持されている。この図4の例では、データファイルAをアクセスするために必要なアクセス場所の情報セキュリティレベルは“A”であり、データファイルBをアクセスするために必要なアクセス場所の情報セキュリティレベルは“C”である場合が示されている。この場合、もしデータファイルA、B双方についてアクセスが許可されている利用者が、携帯情報端末11を情報セキュリティレベル“B”のアクセス場所で操作すると、データファイルBに対するアクセス要求については許可されるが、データファイルAに対するアクセス要求については禁止される。

【0028】次に、図5のフローチャートを参照して、図1のアクセス制御システムの動作について説明する。ユーザが、ある資源へのアクセスを要求し、その結果が得られるまでの流れは次のようになる。

【0029】1. アクセス制御システムは、ユーザがある資源へのアクセスを要求したことを検知すると、イベント待ち状態から抜け（ステップS11）、以下のアク

セス制御動作を行う。

【0030】2. すなわち、まず、アクセス制御システムのユーザ識別認証部111は、ユーザを特定し、場所識別認証部112はユーザのいる場所の情報セキュリティレベルを特定して、結果をアクセス可否判定部113に渡す（ステップS12、13）。

【0031】3. 次に、アクセス可否判定部113は、ユーザ、アクセス場所の情報セキュリティレベル、およびアクセス対象資源の情報を元にアクセス制御リスト115をサーチし、アクセス要求の許可／非許可の判定を行う（ステップS14）。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ116に記録される（ステップS15、16）。

【0032】4. また、アクセス要求を許可した場合には、アクセス制御システムは、ユーザに対して要求された資源を渡す（ステップS17）。以上のように、この実施形態1においては、情報端末11を利用するアクセス場所が特定され、そのアクセス場所の情報セキュリティレベルを使用したアクセス制御が行われる。このため、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加できるようになり、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。

【0033】従って、公共の場所などのようにセキュリティレベルが低い場所では機密性の高い情報へのアクセスは禁止されるが、外出先であっても、セキュリティレベルが高い場所であれば、機密情報にアクセスすることができる。よって、十分なセキュリティを確保しながらユーザの利便を考慮したアクセス形態を実現できる。

【0034】次に、図6乃至図8を参照して、この発明の第2実施形態を説明する。図6には、この発明の第2実施形態に係るアクセス制御システムの実現形態が示されている。第2実施形態のアクセス制御システムは、携帯情報端末11が存在するアクセス場所の情報セキュリティレベルを使用したアクセス制御を行う点については実施形態1と同様であるが、ここでは、携帯情報端末11がサーバ計算機21内の各種資源215に対するアクセスを要求し、そのアクセス可否判定をサーバ計算機21内で行うように構成されている。

【0035】すなわち、アクセス制御システムを実現するための構成要素のうち、携帯情報端末11側には、ユーザ識別認証部121およびアクセス場所識別認証部122が設けられており、サーバ計算機21側には、ユーザ情報検証部211、計算機識別認証部212、場所情報検証部213、アクセス可否判定部214、アクセス制御リスト216、およびアクセスログ217が設けられている。

【0036】次に、図7および図8のフローチャートを

参照して、図 6 のアクセス制御システムの動作について説明する。ここで、図 7 は携帯情報端末 11 側の処理を示し、図 8 はサーバ計算機 21 側の処理を示している。

【0037】ユーザが、ある資源へのアクセスを要求し、その結果が得られるまでの流れは次のようになる。  
1. 携帯情報端末 11 のアクセス制御システムは、ユーザがサーバ計算機 21 内のある資源へのアクセスを要求したことを検知すると、イベント待ち状態から抜け（ステップ S 21）、以下のアクセス制御動作を行う。

【0038】2. すなわち、まず、携帯情報端末 11 のユーザ識別認証部 121 はユーザを特定し、場所識別認証部 122 はユーザのいる場所のセキュリティレベルを特定する。そして、それらの情報を、アクセス要求された対象資源情報とともに、リモートマシンであるサーバ計算機 21 にアクセス要求として送る（ステップ S 24）。

【0039】3. サーバ計算機 21 はそのアクセス要求に回答してイベント待ち状態から抜け（ステップ S 31）、そして、計算機識別認証部 212 は、要求元の計算機を特定し、結果をアクセス可否判定部 214 に渡す（ステップ S 32）。また、ユーザ情報検証部 211 と場所情報検証部 212 は、携帯情報端末 11 から送られてきた情報が正しいかを検証し、結果をアクセス可否判定部 214 に渡す（ステップ S 33、S 34）。

【0040】4. アクセス可否判定部 214 は、ユーザ、アクセス場所のセキュリティレベル、要求元の計算機、対象資源の情報を元に、アクセス制御リスト 216 をサーチし、アクセス要求の許可／非許可を判定する（ステップ S 35）。アクセス制御リスト 216 には、図 4 の情報に加え、各資源をアクセス許可する計算機名が登録されている。これは、複数の携帯情報端末 11 からのアクセス要求に対処するためである。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ 217 に記録される（ステップ S 36、S 37）。

【0041】5. また、アクセス要求を許可した場合には、サーバ計算機 21 は、要求元の携帯情報端末 11 に資源を渡す（ステップ S 38）。

6. 携帯情報端末 11 は、サーバ計算機 21 からのアクセス許可の返答に応じて、サーバ計算機 21 から渡された資源をユーザに渡す（ステップ S 25）。

【0042】この様に、実施形態 2 においても、ユーザがアクセスを要求してきた場所をアクセス可否の判断基準に追加されているので、アクセス場所に応じて、利用できる資源の制限を変えることが可能となる。また、サーバ計算機 21 の利用によって、アクセス可能な資源の量を増やすことができる。さらに、ユーザが直接利用する携帯情報端末 11 の構成が簡素化されるため、小型化／軽量化／低コスト化が図れ、個人が携帯 PC を持ち歩くといったようなモバイルコンピューティングに最適

なアクセス制御システムを構築できる。

【0043】次に、図 9 乃至図 11 を参照して、この発明の第 3 実施形態を説明する。図 9 には、この発明の第 3 実施形態に係るアクセス制御システムの実現形態が示されている。第 3 実施形態のアクセス制御システムは、サーバ計算機 21 から渡された各種資源 135 を保持し、その管理および運用を行うキャッシュ管理部 133 が携帯情報端末 11 に設けられており、ユーザから要求された資源が携帯情報端末 11 内にある場合にはその資源に対するアクセス要求の可否判定を携帯情報端末 11 のアクセス可否判定部 134 で行い、ユーザから要求された資源が携帯情報端末 11 内にない場合にはその資源に対するアクセス要求の可否判定をサーバ計算機 21 のアクセス可否判定部 224 で行う構成である。

【0044】次に、図 10 および図 11 のフローチャートを参照して、図 9 のアクセス制御システムの動作について説明する。ここで、図 10 は携帯情報端末 11 側の処理を示し、図 11 はサーバ計算機 21 側の処理を示している。

【0045】ユーザが、ある資源へのアクセスを要求し、その結果が得られるまでの流れは次のようになる。  
1. 携帯情報端末 11 のアクセス制御システムは、ユーザがある資源へのアクセスを要求したことを検知すると、イベント待ち状態から抜け（ステップ S 41）、以下のアクセス制御動作を行う。

【0046】2. すなわち、まず、携帯情報端末 11 のユーザ識別認証部 131 はユーザを特定し、場所識別認証部 132 はユーザのいる場所のセキュリティレベルを特定して、結果をアクセス可否判定部 134 に渡す（ステップ S 42、S 43）。

【0047】3. アクセス可否判定部 134 は、対象資源が携帯情報端末 11 上にあるか否かをキャッシュ管理部 133 に問い合わせ、キャッシュ検索を実行させる（ステップ S 44）。

【0048】4. 対象資源が携帯情報端末 11 上にあった場合、アクセス可否判定部 134 は、ユーザ、場所のセキュリティレベル、対象資源の情報を元に、サーバ計算機 21 から以前に渡された資源に関するアクセス制御リスト 136 をサーチし、アクセス要求の許可／非許可を判定する（ステップ S 45）。アクセス制御リスト 136 は、図 4 のようなデータ構造を持つ。判定結果は許可／非許可のどちらの場合においても、アクセス制御履歴として、アクセスログ 137 に記録される（ステップ S 46、S 47）。また、アクセス要求を許可した場合には、アクセス制御システムは、ユーザに対して要求された資源を渡す（ステップ S 48）。

【0049】5. 対象資源が携帯情報端末 11 上になかった場合には、携帯情報端末 11 のアクセス可否判定部 134 は、ユーザ、場所のセキュリティレベル、対象資源の情報を、リモートマシンであるサーバ計算機 21 に



アクセス要求として送る（ステップS49）。

【0050】6. サーバ計算機21はそのアクセス要求に  
1 応答してイベント待ち状態から抜け（ステップS6  
1）、そして、計算機識別認証部222は、要求元の計  
算機を特定し、結果をアクセス可否判定部224に渡す  
（ステップS62）。また、ユーザ情報検証部221と  
場所情報検証部222は、携帯情報端末11から送られ  
てきた情報が正しいかを検証し、結果をアクセス可否判  
定部224に渡す（ステップS63、S64）。

【0051】7. アクセス可否判定部224は、ユー  
10 ザ、アクセス場所のセキュリティレベル、要求元の計  
算機、対象資源の情報を元に、アクセス制御リスト226  
をサーチし、アクセス要求の許可／非許可を判定する  
（ステップS65）。アクセス制御リスト226には、  
図4の情報に加え、各資源をアクセス許可する計算機名  
が登録されている。判定結果は許可／非許可のどちらの  
場合においても、アクセス制御履歴として、アクセスロ  
グ217に記録される（ステップS66、67）。

【0052】8. また、アクセス要求を許可した場合には、  
15 サーバ計算機21は、要求元の携帯情報端末11に  
資源を渡す（ステップS68）。

9. 携帯情報端末11は、サーバ計算機21より資源と  
それに関するアクセス制御リストが渡された場合は、キ  
ャッシュ管理部133がその資源およびアクセス制御リ  
ストを携帯情報端末11内に記憶した後、その資源をユ  
ーザに渡す（ステップS50、S51）。

【0053】この様に、実施形態3においても、ユーザ  
がアクセスを要求してきた場所をアクセス可否の判断基  
準に追加されているので、アクセス場所に依じて、利用  
できる資源の制限を変えることが可能となる。また、一  
度利用した資源は、携帯情報端末11上に保存されるの  
で、一般的に通信時間／通信コストのかかるサーバへ計  
算機21の問い合わせ回数を減らすことができる。

【0054】なお、以上の実施形態1～3では、場所識  
別子認証部112、122、132が図2の発信器10  
0を用いてアクセス場所の情報セキュリティレベルを  
特定する場合を説明したが、場所の識別子とその場所の  
セキュリティレベルとの対応関係を示すテーブルを用  
意しておけば、場所識別子認証部112、122、13  
2をそれぞれアクセス場所の識別子だけを検知するだけ  
40 の構成にしても、アクセス場所に依じたアクセス制御を  
行うことができる。

【0055】

【発明の効果】以上説明したように、この発明によれ  
ば、アクセス制御の基準に、アクセス要求してきた「場  
所」の情報を追加することで、制御が細かくできるよう  
になり、モバイルコンピューティングなど、不特定の  
場所からの各種資源へのアクセスといった状況において  
も、セキュリティを確保しながら、ユーザの利便を増す  
ことが可能となる。

【図面の簡単な説明】

【図1】この発明の第1の実施形態に係るアクセス制御  
10 システムが適用されるモバイルコンピューティングシ  
ステム全体の構成を示すブロック図。

【図2】同第1実施形態のアクセス制御システムにおけ  
るアクセス場所に関する識別および認証処理の原理を説  
明するための図。

【図3】同第1実施形態のアクセス制御システムで使用  
されるセキュリティーレベル発信器から発生されるセキ  
ュリティーレベル信号の内容とセキュリティレベルの高  
低との対応関係を説明するための図。

【図4】同第1実施形態のアクセス制御システムで使用  
20 されるアクセス制御リストの構成を示す図。

【図5】同第1実施形態のアクセス制御システムのアク  
セス制御処理の手順を示すフローチャート。

【図6】この発明の第2の実施形態に係るアクセス制御  
システムの構成を示すブロック図。

【図7】同第2実施形態のアクセス制御システムのアク  
セス制御処理の手順の一部を示すフローチャート。

【図8】同第2実施形態のアクセス制御システムのアク  
セス制御処理の手順の残りの一部を示すフローチャー  
ト。

30 【図9】この発明の第3の実施形態に係るアクセス制御  
システムの構成を示すブロック図。

【図10】同第3実施形態のアクセス制御システムのアク  
セス制御処理の手順の一部を示すフローチャート。

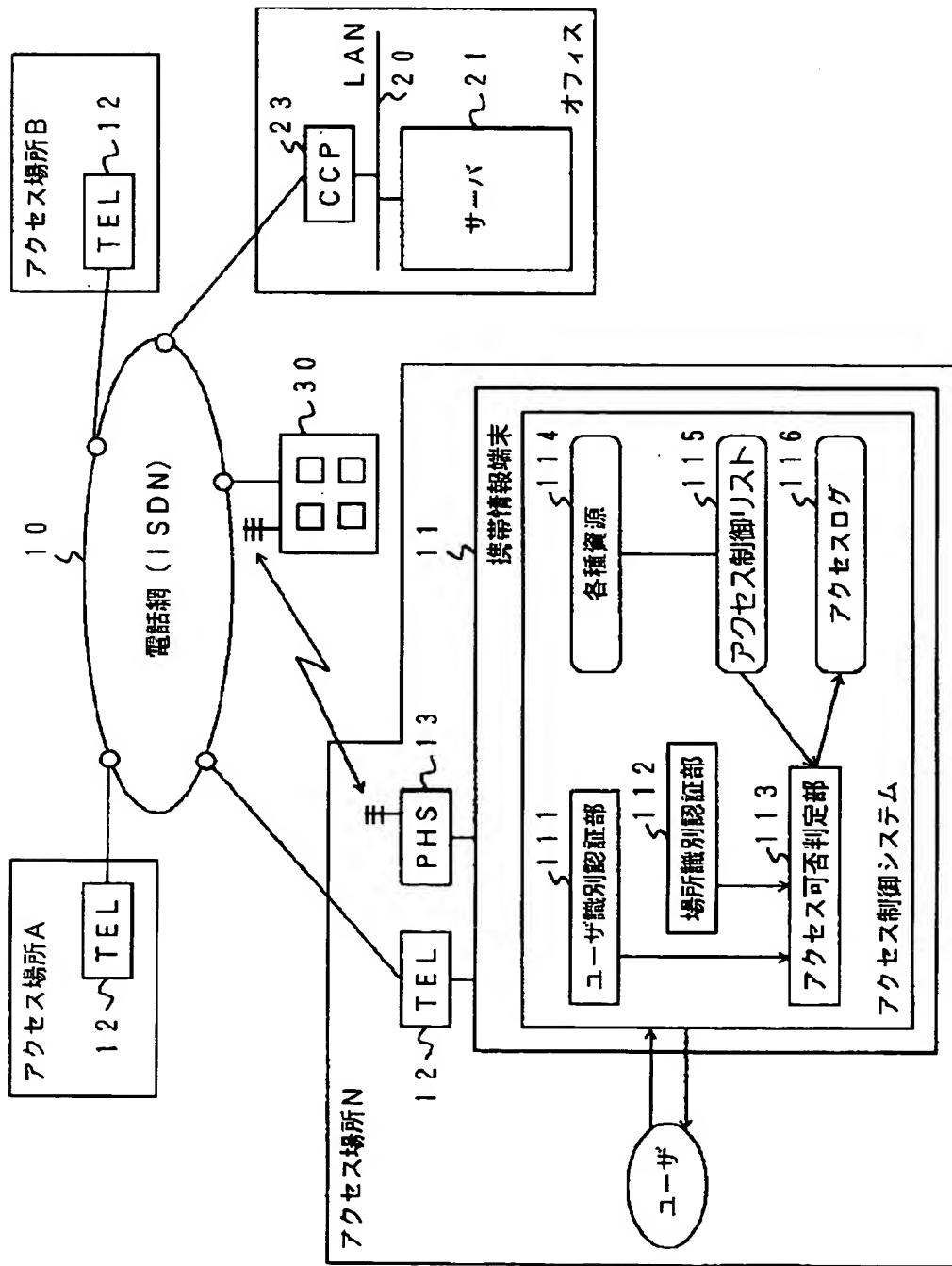
【図11】同第3実施形態のアクセス制御システムのアク  
セス制御処理の手順の残りの一部を示すフローチャー  
ト。

【符号の説明】

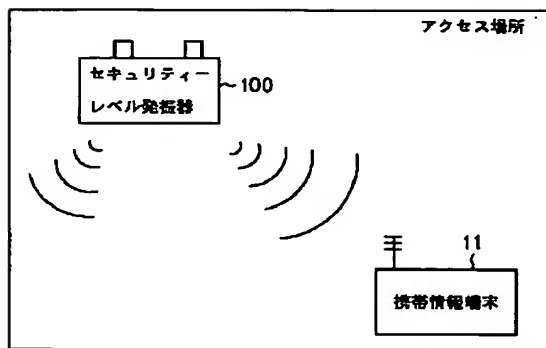
11…携帯情報端末、21…サーバ計算機、111、1  
21、131…ユーザ識別認証部、112、122、1  
32…アクセス場所識別認証部、113、134、21  
4、224…アクセス可否判定部、115、136、2  
16、226…アクセス制御リスト。



【図1】



【図 2】



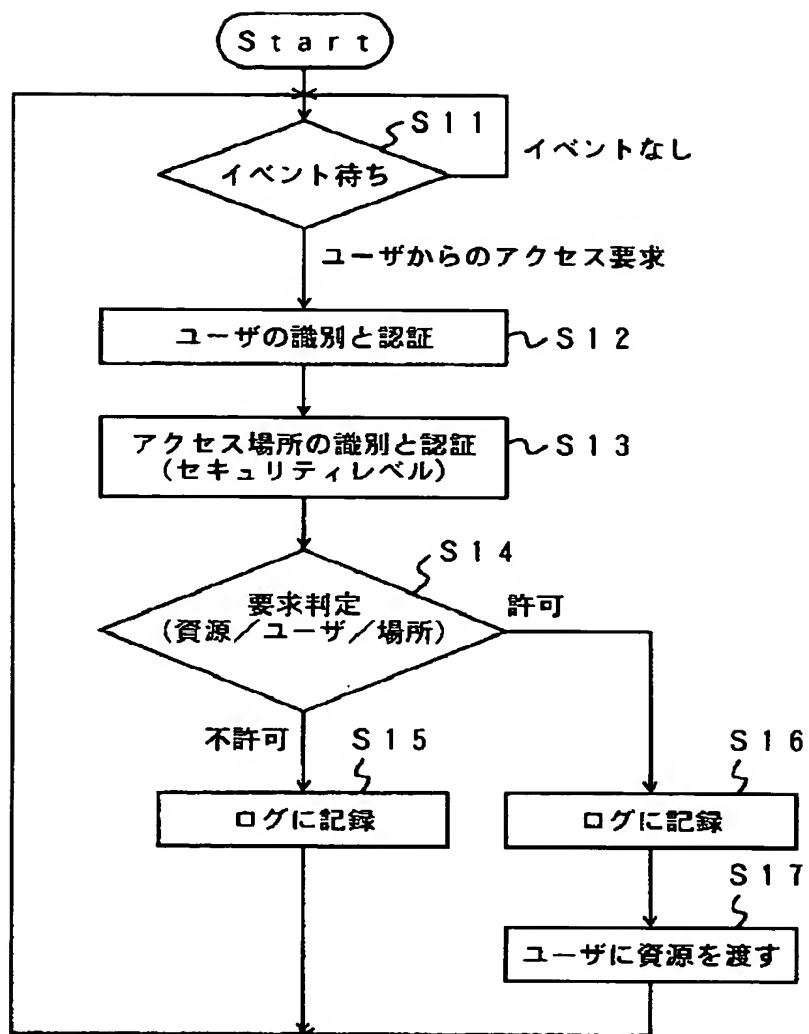
【図 3】

セキュリティレベル信号	セキュリティレベル
A	高
B	↓
C	
D	
E	
F	低

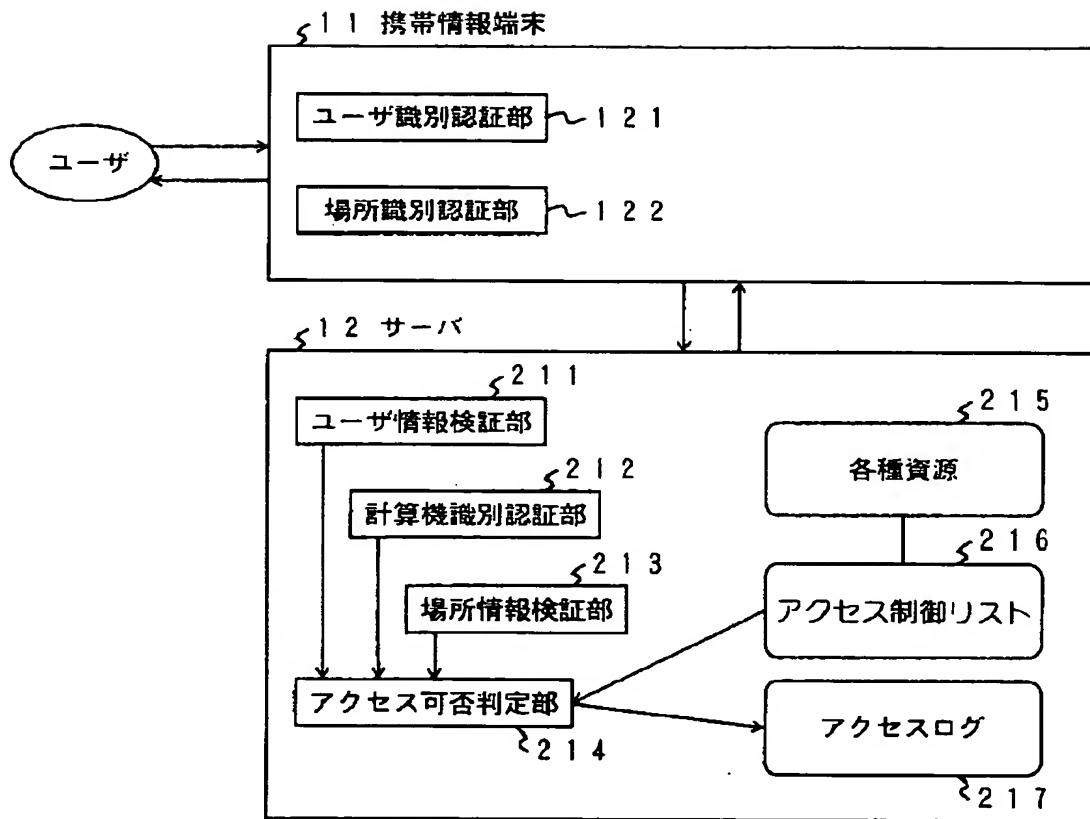
【図 4】

資 源	ユーザ名/グループ名	セキュリティレベル
データファイルA		A
	⋮	
データファイルB		C
⋮	⋮	⋮

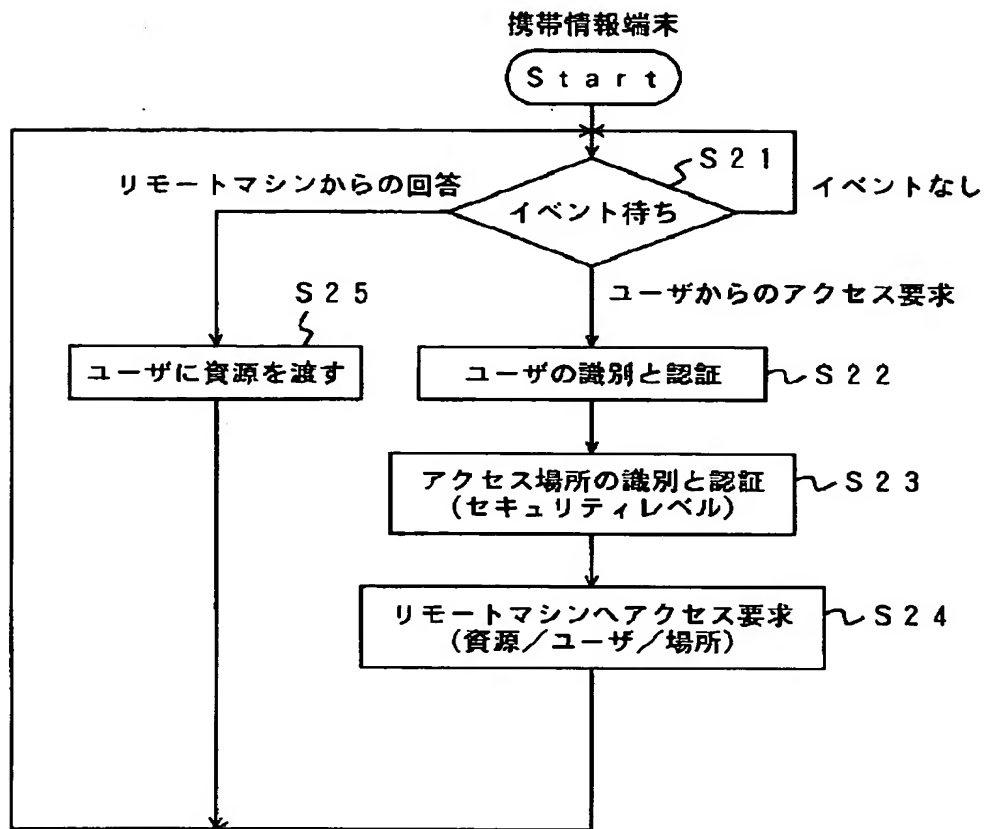
【図 5】



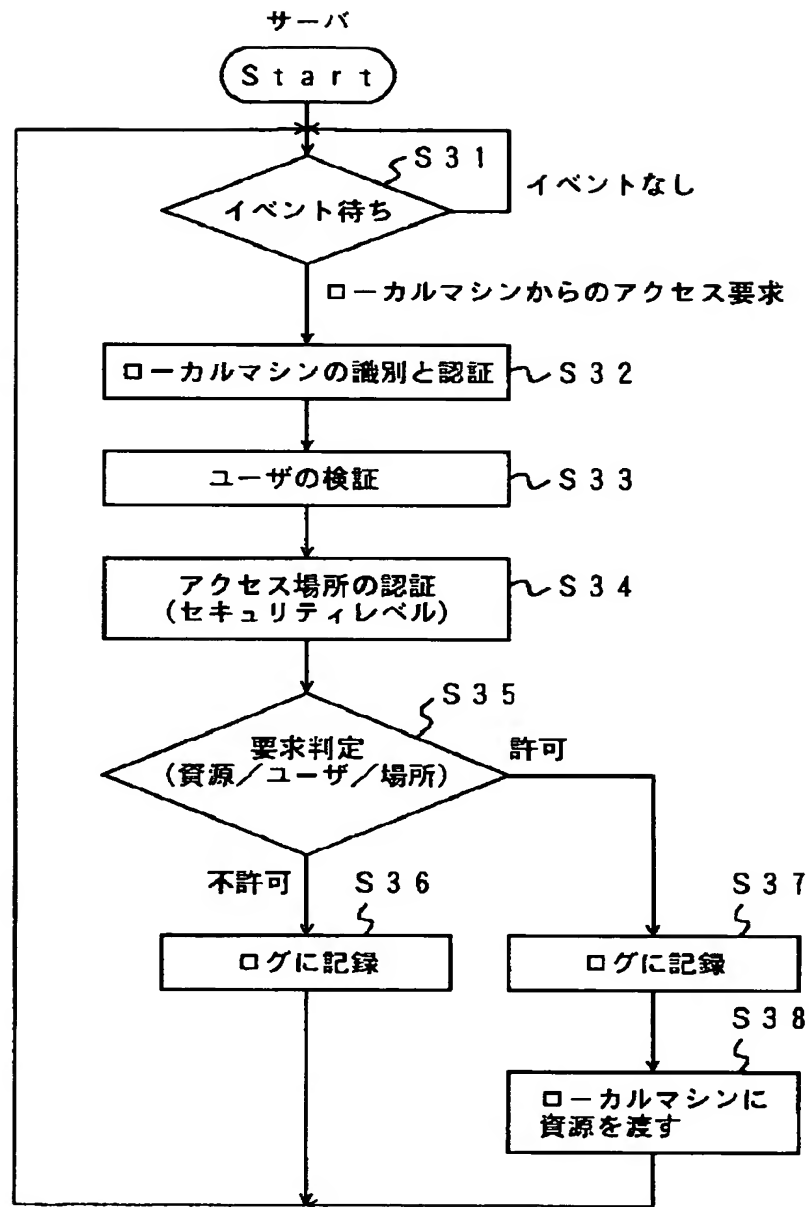
【図 6】



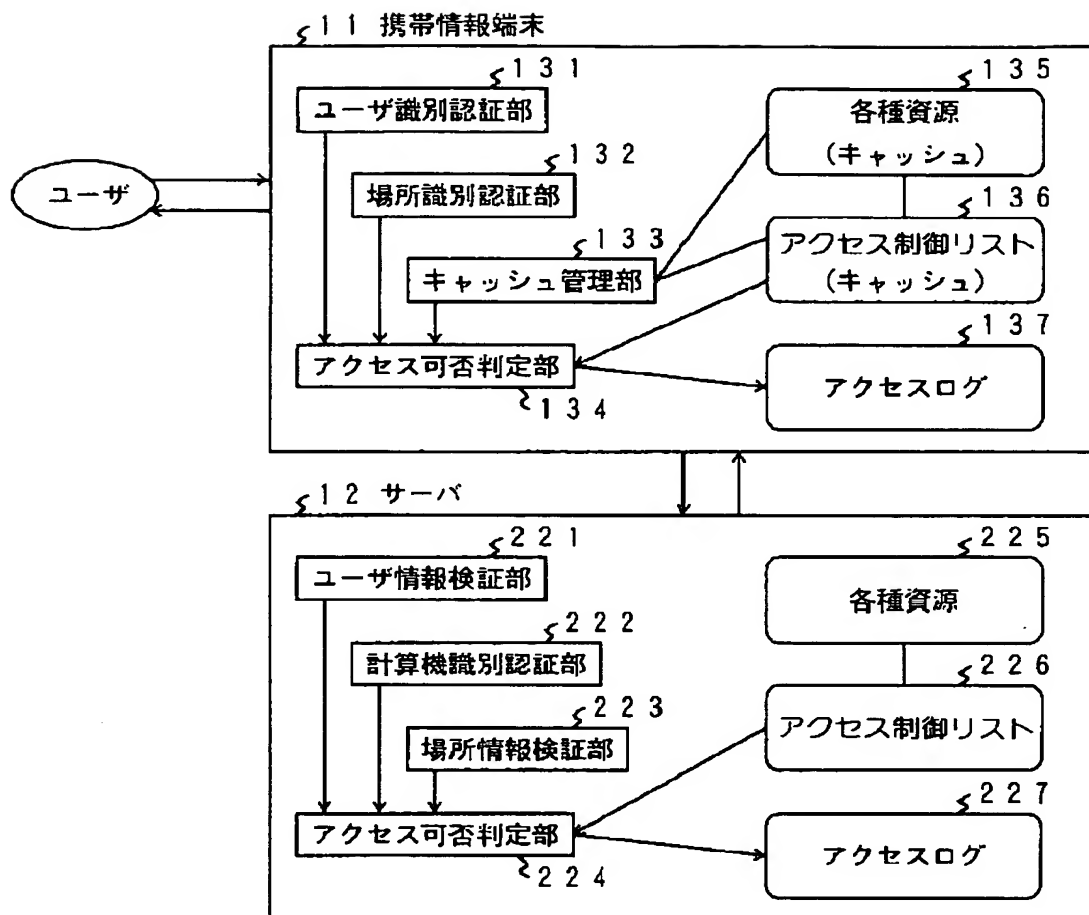
【図 7】



【図8】

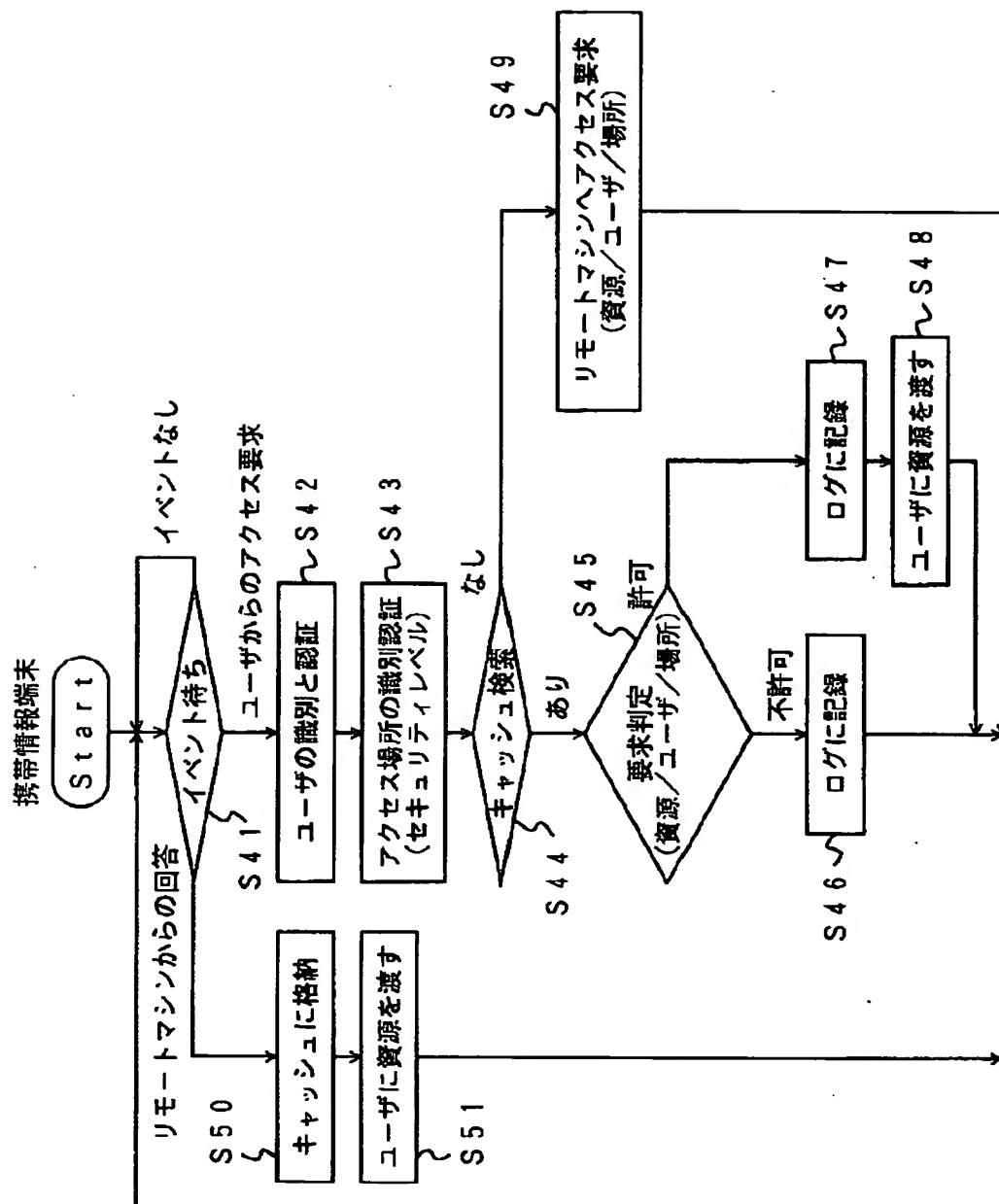


【図9】





【図10】



【図 11】

